

UNCLASSIFIED

NAVAL WAR COLLEGE
Newport, R. I.

JOINT MILITARY OPERATIONS RESEARCH PAPER

"Information Warfare (IW) and Command and Control Warfare (C2W) for the Naval Expeditionary Task Force Commander"

by
Martin P. Kurdys
CDR, USN
Seminar 14

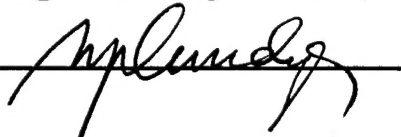
DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations

The contents of this paper reflect personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy

Signature



8 April 1996

DTIC QUALITY INSPECTED 4

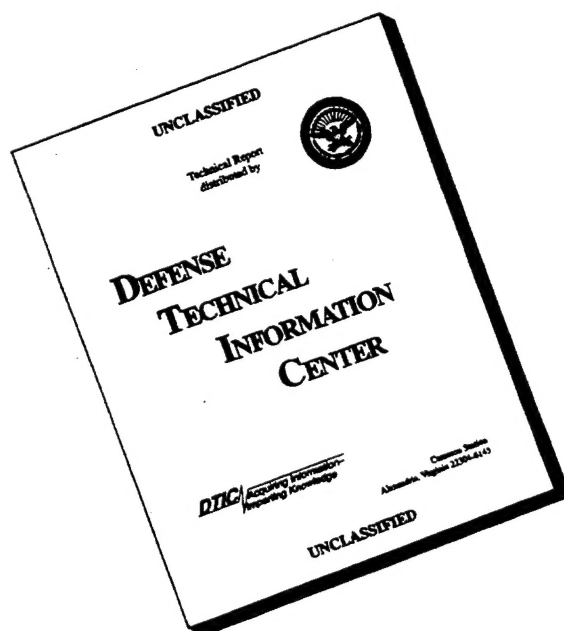
19960815 056

Faculty Advisors

Rick Stevens, CDR, USN, JMO Dept

Professor Mike Handel, Strategy and Policy Dept.

DISCLAIMER NOTICE



**THIS DOCUMENT IS BEST
QUALITY AVAILABLE. THE
COPY FURNISHED TO DTIC
CONTAINED A SIGNIFICANT
NUMBER OF PAGES WHICH DO
NOT REPRODUCE LEGIBLY.**

UNCLAS

Security Classification This Page

REPORT DOCUMENTATION PAGE

| | |
|---|---|
| 1. Report Security Classification: UNCLASSIFIED | |
| 2. Security Classification Authority: | |
| 3. Declassification/Downgrading Schedule: | |
| 4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED. | |
| 5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT | |
| 6. Office Symbol: C | 7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207 |
| 8. Title (Include Security Classification): Information Warfare ^(IW) Command and Control Warfare ^(C2W) for the Naval Expeditionary Task Force Commander (U) | |
| 9. Personal Authors: Martin P. Kurdys, CDR, USN | |
| 10. Type of Report: FINAL | 11. Date of Report: 8 Apr 96 |
| 12. Page Count: 24 | |
| 13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy. | |
| 14. Ten key words that relate to your paper: Information Warfare Command and Control Warfare Naval Expeditionary Forces | |
| 15. Abstract: The bottom line to a Commander of a Naval Expeditionary Force is how Information Warfare (IW) and Command and Control Warfare (C2W) can increase the operational effectiveness of the force responding to a contingency. To get there, one must examine the national strategic role of IW, the traditional role of the Naval Expeditionary Force, and the operational role of C2W. From these, an operational level approach to IW/C2W can be developed that is both consistent with strategy and doctrine and useful to the Commander of a Naval Expeditionary Force. | |

| | | | |
|---|-----------------------|---------------------|------------|
| | | | |
| 16.Distribution / Availability of Abstract: | Unclassified X | Same As Rpt | DTIC Users |
| 17.Abstract Security Classification: UNCLASSIFIED | | | |
| 18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT | | | |
| 19.Telephone: 841- 643 6461 | | 20.Office Symbol: C | |

Security Classification of This Page Unclassified

Information Warfare (IW) and Command and Control Warfare (C2W) for the Naval Expeditionary Force Commander

"Information War, Command and Control Warfare, Cyberspace, Netwar...Just tell me how this helps me put iron on the target!!"

The plethora of books, articles, publications and instructions describing the supposedly new (and some say revolutionary) concept of information warfare has been accompanied by dire predictions about the future, imaginatively constructed warfare paradigms, anxious hand-wringing, and a mad scramble for power and money. As each interest group inside the Washington Beltway debate the implications of war in cyberspace, and exactly which flea should own the dog, operational commanders are left to wonder about the real relevance of IW/C2W to Naval crisis/contingency operations.

Introduction

The bottom line to a Commander of a Naval Expeditionary Force is how Information Warfare (IW) and Command and Control Warfare (C2W) can increase the operational effectiveness of the force in responding to a crisis or contingency. To get there, one must examine the national strategic role of IW, the traditional role of the Naval Expeditionary Force, and the operational role of Command and Control Warfare (C2W). From these, an operational level approach to IW/C2W can be developed that is both consistent with strategy and doctrine and useful to the

Commander of a Naval Expeditionary Force.

The Strategic Setting

Since the end of the Cold War, both political and military strategists have sought to develop an "enlightened" approach to the U.S. role in the new world (dis)order. U.S. national security strategy in each region of the world can be said to flow from three broad

**"Know the enemy and know yourself;
in a hundred battles you will never be
in peril."**

**—Sun Tzu, "The Art of
War"**

goals: sustaining our security with military forces that are ready to fight, bolstering America's economic revitalization, and promoting democracy abroad.¹ President Clinton's National Security Strategy (NSS) delineates an *integrated regional approach*, and the National Military Strategy (NMS) formulates two military objectives: promoting stability and thwarting aggression.² A component of the strategy, "to fight and win," identifies as a sub-component principle to "help dominate combat operations by winning the information war."³

Information Warfare (IW) has reached megastar status as the new Washington D.C. buzzword. Accordingly, IW departments, commands, and "experts" have spread throughout the Military-Industrial complex like cancer, each with its own agenda, predictions about the future of warfare, and unique bid for money and power. Trendy new weapons, such as those contained in Appendix A, are some of the precision guided munitions of IW, and if the futurists are to be believed, provide a key element of the so-called Revolution in Military Affairs (RMA). There are ^{some} around 25 Boards, Forums, Committees, Working Groups, Subcommittees, Task Forces, and

¹ "A National Security Strategy of Engagement and Enlargement." (Washington DC: The White House, February 1995), p. i.

² "National Military Strategy of the United States of America: A Strategy of Flexible and Selective Engagement." (The Joint Chief of Staff, The Pentagon, Washington DC, February 1995), p.1.

³ Ibid., p. 4.

Councils established at the National level for IW, over 230 "key" published policy documents, implementation standards, guidelines and procedures, and over 160 "key" points of contact in the Executive Branch and the Department of Defense for Information Warfare.⁴ The American Civil Liberties Union, constitutional scholars, business leaders, and Executive Branch General Counsels wrangle over the implications of the Right to Privacy versus securing Federal Information and Intelligence Systems Security versus international law, public law, and applicable U.S. Codes. However, throughout the great debate over a national information warfare strategy, three things remain unarguable:

(1) "There is a potentially significant asymmetry in employable means between the adversary and the United States. A potential opponent can often use by any means technically available [the means] to penetrate or exploit or disrupt and deny U.S. information systems---in peace as well as war. The U. S. warfighters, however, may have significant constraints placed on them by law and regulation, limiting their actions."⁵

(2) There will not be a consensus on a National Information Warfare Strategy anytime soon.

and, (3) the "new and revolutionary role" for the Commander of the Naval Expeditionary Task Force in IW/C2W seems, at best, unclear.

Getting to the Bottom Line

The Department of Defense has been in the business of electrical and electronic information collection, analysis, and manipulation for years. Besides monitoring enemy electronic emanations (electronic intelligence or ELINT) and communications signals (communications intelligence or COMINT), the business also included active measures to confuse and disrupt

⁴ "Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance." (A Research Report for the Chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Directorate, Joint Staff, The Pentagon. Prepared by Scientific Applications International Corporation (SAIC), Telecommunications and Networking Systems Operation, dated 4 July 1995. Contract No. MDA903-93-D-0019).

⁵ Ibid., p.2-65.

enemy command and control. Highly classified, owing to the sensitivity and fragility of sources and techniques, the Naval Security Group was the Chief of Naval Operations agent for SIGINT operations in support of Navy operations, and was the Navy's Service Cryptologic Element (SCE) representative to the National Security Agency (NSA). Active measures are also highly classified in that often they are "silver bullets" that can be fired once--the enemy will know how you did what you did as soon as he sees it.

Proceeding from the National Security Strategy to the development of an operational level plan for IW/C2W might at first glance appear an impossible task, given the expanse of grand strategies intrinsic to the Clintonian "Engagement and Enlargement" (and some critics say Engorgement) strategy. Implicit therein are elements of primacy, selective engagement, and collective security. Primacy would seek to prevent the emergence of any power that threatened our international hegemony, suggesting one set of target countries. Selective engagement suggests peace among great powers. Considering this strategy's implications in terms of information warfare "target countries," the list would have to be broadened to include those countries that could either cause great powers to go to war or draw the United States into a war with great powers that was of sufficient ferocity to threaten our security. Cooperative security is best understood in the context of peace, not power. Whereas primacy and selective engagement tend to define enemies, cooperative security defines allies. It's proponents assume that the world is a safer place since the end of the Cold War, and we should now focus our energies in the pursuit of world peace, rather than the preparations for war. It implies preventive, rather than corrective, strategies, "giving much more attention to organizational reform, particularly within the United Nations."⁶ It suggests that through cooperation the economic and industrialized powers can prevent intrastate conflict and promote world peace. Postulating target countries for information warfare is difficult. Cooperative security seems to assume that the industrialized, economically powerful nations are somehow inherently stable, and that intervention would be

⁶ Gareth Evans, "Cooperative Security and Intrastate Conflict," Foreign Policy, No. 10, Fall 1994, p.3.

limited to within Tofflers' First and Second wave states.⁷ Thus, all the states discussed in the selective engagement strategy above would be valid, as would practically every other country, given the circumstances of emergence of an unstable leader, fascist religious/political/ethnic group, or international behavior in violation of humanitarian concerns.

All this notwithstanding, and considering ~~that~~ the National Security Agency's (NSA) national strategic role in signals protection and exploitation, an elegant scheme for IW emerges that is both fitting and consistent with the National Security Strategy and the National Military Strategy, in keeping with the strategic and operational levels of war, using an *integrated regional approach*.

"Information Warfare (IW) is a *national strategy* that employs all the tools of national power to create a competitive advantage at the national strategic level."⁸ In other words, attacking everything that is used to store, transmit, or analyze all the types of information necessary to make decisions relevant to the political, economic, and military well-being of a state. Given this definition for IW, and using the three principles of attack, protect, and exploit as the basis for planning⁹, an approach can be designed to produce at the regional CINC level, a set of strategic Information Warfare Plans (IWP's): each IWP to be Operations plan (OPLAN) or concept plan (CONPLAN) specific, containing a comprehensive description of an individual country's information infrastructure--political, economic and military. It would include:

- (1) military sensors and information systems, radio and television C2 architecture, telephone system architecture (both domestic and international), commercial banking and investment network architecture, and electrical power architecture (including grid breakdowns),
- (2) the most detailed hardware and software descriptions of commercial and domestic

⁷ Alvin and Heidi Toffler, "War and Anti-War: Survival at the Dawn of the 21st Century," (New York: Little, Brown, and Company, 1993), p. 246.

⁸ Norman B. Hutcherson (LTC/USAF), "Command and Control Warfare: Putting Another Tool in the Warfighter's Data Base," (Maxwell AFB, AL: Air University Press, 1994), Chapter 1.

⁹ see OPNAVINST 3430.25, "Information Warfare and Command and Control Warfare", 1 April 1994.

network in use on each,

(3) the target country (or countries') signals intelligence (SIGINT) capability and architecture, electronic warfare capabilities, intelligence capabilities (both civilian and military), as well as a political and psychological warfare assessment keyed to specific political, socioeconomic, ethnic, and/or religious vulnerabilities, and

(4) a protection strategy for U.S. information systems.

This plan, produced by the staff of the regional Unified Commander (or CINC), supported by NSA in concert with the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the Defense Information Systems Agency (DISA), Commander-in-Chief, Special Operations Command (USCINCSOCOM (for the Psychological Operations (PSYOP) portion), and the Department of State, would serve as the basis for implementing the tools of national power to create a competitive advantage. Highly classified, and continuously updated, it would be available in its entirety to only key elements of National Command Authorities and the regional CINC, and would also include legal, regulatory and policy guidance developed as part of a National Information Strategy developed by the Information Warfare Executive Board (IWEB) (see Figure 1).

| PLANNING LEVEL | PRODUCT |
|---|---------------------------------------|
| NATIONAL LEVEL (Strategic) Information Warfare Executive Board (IWEB) (includes DepSecDef as Chair, plus DDCL, VCJCS, DirDISA, DirNSA, DirDIA, USD(P), USD(A&T), Comptroller, General Counsel, NSC rep, and ASD(C3I) | National IW Strategy |

| | |
|---|-----------------------------|
| REGIONAL CINC LEVEL (Strategic/Operational) Warfighting CINC IW/C2W Organization (VCINC, J3, IW/C2W Officer, J6, plus J2 and General Counsel) supported by NSA, DISA, CIA, DIA, SOCOM, DepState. | Regional IW/C2W Plan |
| NAVAL EXPEDITIONARY FORCE (Operational Level) NEF C2W Officer (approved by Commander, N3, supported by N6, N2, and JAG) | Operational C2W Plan |

Figure 1. IW/C2W Planning Architecture

The Naval Expeditionary Force and the Operational Level of War

The White Paper "...From the Sea", signed by the Secretary of the Navy, the Chief of Naval Operations, and the Commandant of the Marine Corps in 1992, defined the Naval Service strategic blueprint for executing the National Security Strategy and the National Military Strategy, and identified key operational capabilities required for execution as Command, Control and Surveillance, Battlespace Dominance, Power Projection, and Force Sustainment. The refined maritime strategic focus contained in the 1994 "Forward...From the Sea" accentuated forward engagement by Naval Forces, describing how and when Naval Forces are to be used, giving hard examples of the flexibility of Naval Forces. Subsequently, the Naval Doctrine Command produced doctrine describing the capabilities, limitations and Joint Operations support, identifying the Naval Expeditionary Force as the core group at the operational level of war, and Space and Electronic Warfare (SEW) as a supporting warfare task. IW/C2W has replaced SEW in the operational lexicon, and OPNAVINST's 3430.25 and 3430.26 describe IW as strategic and C2W as operational/tactical. The operational level of war is defined in Joint Pub 1-02 as

"The level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing operational objectives needed to accomplish the strategic, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events."

In an attempt to translate strategic IW objectives into a set of tasks for the operational commander, Charles E. Heimach of Anser, under contract to the Secretary of the Air Force for Acquisition, produced an IW strategy to operational task breakout as a guide to planning an Infowar campaign "...as an integrated military action covering all information activities that contribute to the success or failure of a conflict."¹⁰ An interesting approach that straddles the strategic/operational line, a portion of the framework is contained in Appendix B, and it provides insight into the bridge between strategic IW and C2W on the military operational level. Given enough time, money and contractors, this framework could be further tailored to each Unified CINC, providing the strategic-operational bridge for broad based IW/C2W in his or her theater.

However, the Naval Expeditionary Force Commander, often first on the scene during crisis/contingency operations, as in the Persian Gulf, Somalia, and the Adriatic, is responsible for developing a plan that fits into the operational scheme, and is consistent with the operational design and the principles of war that can be easily integrated into the Joint Operations Order upon the establishment of a Joint Task Force (JTF).¹¹ Just as the supporting task of intelligence should support the operational scheme, be consistent with the principles of war, and provide an elegant extension to the time-phased force deployment or TPDF, so should the C2W Plan, incorporating all of the elements of operational art.¹²

¹⁰ Charles E. Heimach, "Regional Infowar Campaign: Strategy to Task Breakout." (ANSER: Arlington, Virginia, 1995), p.i.

¹¹ Those principles being Mass, Objective, Offensive, Surprise, Economy of Force, Maneuver, Unity of Command, Simplicity, and Security.

¹² Simultaneity and Depth, Anticipation, Balance, Leverage, Timing and Tempo, Operational Reach and Approval, Forces and Functions, Arranging Operations, Center of Gravity, Direct versus Indirect, Decisive Point, Culmination, and Termination.

The C2W Plan should include the same elements, and consistent with other operational functions, complement the achievement of synchronization in the operations plan as a whole. In other words, there should be a synergy in the employment of air, surface and subsurface Electronic warfare (EW) assets, cryptologic assets, deception, psychological operations (PSYOP), operations security (OPSEC), and communications security (COMSEC) plans, in simultaneity and depth, anticipating enemy operations, in a balanced manner. Own force capabilities should be concentrated against enemy weaknesses, with the timing and tempo consistent with own force operational reach, forces and functions, thereby arranging C2W operations against direct and indirect attack on enemy centers of gravity. Constant reevaluation of the C2W Plan is necessary as own forces approach decisive points and culmination, consistent with achieving one's objectives and war termination strategy. *Put simply, it should provide the operational commander the where, how and why of operational Command and Control Warfare, describing the positioning of reconnaissance, surveillance, and electronic warfare assets to maximize their effective support to operational fires, providing the operational commander a cognitive display of enemy and own force C2.*

The Command and Control Warfare Plan (C2WP)

"...Command and Control Warfare (C2W) is the military strategy that seeks to establish an information advantage by focusing on the C2 decision-making capabilities of both friendly and adversary forces" [at the military operational and tactical level of war].¹³ At the *operational/tactical* level, the C2W Plan should be an appendix to Annex C (Operations) of any Naval Expeditionary Force Commander's operations order (OPORD), and would provide the foundation for the destruction/neutralization of C2 targets, and all electronic warfare, military deception, psychological, and operational security operations (Figure 2).

The CINC's general, regional IW/C2WP could be tailored by the C2W organization of the Naval Expeditionary Force into a crisis/contingency specific C2WP, based on control of the

¹³ Norman B. Hutcherson (LTC/USAF), "Command and Control Warfare: Putting Another Tool in the Warfighter's Data Base." (Maxwell AFB, AL: Air University Press, 1994), Chapter 1.

electromagnetic spectrum to our advantage and the enemy's disadvantage. Rather than organize on the philosophical "pillars" of C2W theory, which are often used to describe C2W, it's more useful to consider three distinct operational considerations: Exploitation/Surveillance, Protection, and Attack.¹⁴

The **exploitation/surveillance** section of the C2W plan can provide a graphical display of nodal analysis, propagation modeling, technical data, activity histograms (electronic and communications emanations over time), target attributes (read imagery), suggested exploitation areas, and signals exploitation equipment indigenous to the force. This set of graphics, window-based, allows the tactical decision-maker to focus on any single area of interest—for instance, a particular air defense site. By "clicking" on that site on a 3-D geographical display, additional information can be attached, including time-based activity histograms (thus making it essentially a "4-D" display), imagery, and technical details relevant to the site.

| C2W Plan | | |
|--|---|--|
| <ul style="list-style-type: none"> -Comprehensive description of individual country information infrastructure. -Provides foundation for planning surveillance, reconnaissance, signals intelligence (SIGINT), destruction/disruption of enemy C3, electronic warfare, military deception, PSYOPS, and operational security (SIGSEC and COMSEC). -Integrates applicable elements of strategic IWP into the operational level of planning. | | |
| Exploitation/Surveillance <ul style="list-style-type: none"> -Graphical Display -Nodal analysis -RF Propagation modeling -Tech Data -Histograms -Attributes (imagery) -Exploitation areas/equip/ assignments | Protection <ul style="list-style-type: none"> -Graphic Display -Vulnerability assessment -Own Force Electronic Signature -Adversary EW/SIGINT capabilities -Protect/Detect/React Strategy | Attack <ul style="list-style-type: none"> -Specific RF Propagation Modeling for Season, Time, Terrain -Activity Histograms -"Herding" Assessment |

Figure 2. Regional/Contingency C2W Plan

¹⁴ The philosophical pillars are most often discussed as Electronic Warfare, PSYOP, Operations Security (OPSEC), Deception and Destruction.

Propagation modeling gives the decision maker a "view" of the sensor radio frequency pattern of the site, as modified by geography and meteorology, and also provides insight into the optimum positioning of collection assets. Nodal analysis graphics serve to highlight information wealth and paucity concerning that sites command and control connectivity. Included in this section, albeit at a higher classification level, is the cryptologic and electronic warfare exploitation strategy, based on propagation modeling, service/platform SIGINT collection capability, data base content (e.g. what "holes" exist in national and regional SIGINT data bases), target priority, and individual platform operating area. This element of the C2W Plan is also dynamic, as priorities feed collection strategy, and as collection strategy is translated into tasking, and as tasking/collection continues to satisfy respective priorities. Further, unit location and individual equipment capabilities will continuously change, adding to the dynamic. A continuously tuned exploitation strategy allows for precise collection management, eliminates duplication of effort, focuses SIGINT and EW operators on specific objectives, provides a vehicle for methodical signals search and development in pre-crisis and crises phases, and facilitates synergistic collection. The second element of this section can contain the target specific PSYOP plan.¹⁵ The essentiality of this section was demonstrated beyond a shadow of a doubt in the Persian Gulf crisis, and PSYOP ensures the enemy remains deep within the so called "fog of war", while providing much of the basis for designing own force deception operations.¹⁶ Thus flows nicely the third element of this section, deception operations (OPDEC), which seeks to hide own force disposition, size and intentions from the enemy, while maximizing confusion on his part. The OPDEC plan should be keyed to not only force size and capability, but to each phase of the operation, whether it is a Non-combatant Evacuation Operation (NEO) or a Major Regional Crisis (MRC), which may

¹⁵ Using the Joint Maritime Command Information System (JMCIS), this can be imported electrically (via the embedded JDISS capability) from the U.S. Army's 4th PSYOP Group. This element serves to highlight a key consideration: the C2W Plan is a joint document that spans inter- and intraservice lines — no one "owns" IW/C2W, but rather, everybody has a valid and unique contribution. Tasking to produce this section would be accomplished via the theater CINC and via USCINCSOCOM, who owns DoD PSYOPS assets.

¹⁶ see Jefferey B. Jones (COL/USA), "Psychological Operations in Desert Shield, Desert Storm, and Urban Freedom," Special Warfare, July 1994, pp.22-29.

include halting the invasion, building up combat power, and decisively defeating the enemy.¹⁷

The **protection** section of the plan provides the decision maker with a comprehensive vulnerability assessment of own forces. It includes a 3-D geographical display of own force radio frequency propagation, based on the force communications plan, location/capabilities of adversary SIGINT sites, and information regarding own force electronic signatures. This section should also include a risk management strategy, like the one suggested by Ron Knecht of SAIC¹⁸, incorporating protect, detect and react planning, in which the force protection plan is a dynamic that is continually realigned in the context of the Communications Plan, the Joint Restricted Frequency List (JRFL), and detections of enemy intrusion or interference.

The final section of the plan, **attack**, contains propagation modeling based on season, time, and terrain keyed to the precise time window for implementation of the OPORD. Collection results and SIGINT and electronic order of battle (EOB) data bases built up to this point are key to developing this section. Again, the section is dynamic, and as activity histograms change based on soft or hard kill, attack strategy will be updated. Attack plans must be guided by two, sometimes opposing goals: disabling/disrupting enemy command control communications and "herding" enemy communications into a spectrum exploitable for intelligence. Again, the value of a cognitive display to the decision-maker, showing nodal analysis, battle damage, and residue command and control and electronic warfare capability is obvious. The decision-maker must be aware from the outset the consequences of attack, and may wish to structure the precise targets to confuse and confound in some instances, and simply destroy in others. Special weapon use, as well as decisions regarding C2W related special warfare direct action missions, could be determined by the C3 technical data and imagery contained herein.

A final consideration is that the C2W Plan be divided into three basic classification levels: SCI, GENSER Secret, and releasable to coalition forces. Predicating these three levels will allow

¹⁷ phase description from Les Aspin, Secretary of Defense, Report on the Bottom-Up Review, (Washington, DC, October 1993).

¹⁸ Ron Knecht, "Thoughts on Information Warfare," (Science Applications International Corporation, June 1994), p.32.

fine tuning of the plan based on previously negotiated security agreements with allies.

An Operational Approach

From the above, it is apparent that developing comprehensive IWPs and C2WPs for all the target countries mentioned above would consume tremendous resources and be predicated on some consensus on information

"Everybody's talkin' 'bout the new sound; funny, but it's still rock and roll to me."

—Billy Joel

warfare policy at the national level. A pragmatic approach is to define a small group of countries in which the most immediate propensity for military operations exists, articulate information warfare intelligence requirements to the National Intelligence organization to satisfy collection not within the realm of regional military forces during routine peacetime operations, and design theater surveillance and reconnaissance plans commensurate with satisfaction of IW/C2W goals.¹⁹ During peacetime operations, routine reconnaissance and surveillance by service component assets should be ongoing to develop the data bases to support the C2WP, and consolidated at the regional CINC.

In the Navy's case, the most attractive alternative for a coordination point for such an effort, from the point of view of currently available personnel, expertise, information systems, and inherent security, is the Numbered Fleet C2W Ship Signal Exploitation Spaces (SSESs) afloat and at the Cryptologic Shore Support Activities (CSSAs) ashore. From these two entities, regional data bases can be developed and merged, and with collocated intelligence, communications, and electronic warfare personnel and expertise, be produced into the C2W Plans discussed above. With the advent of JMCIS, with its embedded JDISS/MOSAIC/INTELINK capability, C2W Plans can be rapidly exchanged with tactical users, both Navy and other service, as well as with supporting National Intelligence agencies in real time, supporting development up the chain of regional, strategic IW/C2W Plans at the CINC level. The proliferation of compatible 3-D

¹⁹ in the European Southern Region, for example, one might consider Bosnia/Serbia/Croatia, Libya, and Algeria.

mapping softwares, found in many NSA software tools, makes this synergy complete, ensuring the easy transfer of data with other services, the national intelligence system, and the regional CINC Staff.

The Navy is the only service that has retained professional cryptologists in a restricted line career field who have the required expertise in communications, security, electronic intelligence, and communications intelligence required for information warfare modeling. The Naval Security Group has also been designated as the executive agent for all Navy electronic warfare and IW/C2W training, and its field stations are nearly always located near Naval Computer and Telecommunications Commands. The Navy's investment in a specialized cryptologic career field can show a real payoff in information warfare, and may prove to be the core of operational planning for C2W for the Naval Expeditionary Task Force. Direct support of operational forces has been a traditional role for Naval Security Group, and their "embedded in the force", vision ensures they remain responsive to the goals and needs of the operational commander.²⁰ Further, their traditions in SIGINT, SIGSEC, ELINT analysis, special intelligence communications bespeak an ability to communicate with the Naval commander in real time, thus providing the planning support commensurate with the operational planning requirements of Command and Control Warfare at the Naval Expeditionary Force level. And most importantly, the success of cryptologic Direct Support Elements as a force multiplier, and the fact that they remain in demand by deploying CVBG and MARG commanders, means that the support they provide has broken through the "Green Door," allowing direct translation into the operational planning process.

Finally, some concluding thoughts:

(1) The proliferation of telecommunications links and computer-to-computer digital communications used by both military and commercial clients has highlighted the SIGSEC and SIGINT challenge.²¹

(2) The Naval Expeditionary Commander need not reorient traditional warfighting (read operational fires) around some new shipboard space filled with computer hackers who will conduct war in cyberspace, flitting hither and yon, injecting viruses and time-bombs via an

²⁰ in the European Southern Region, for example, one might consider Bosnia/Serbia/Croatia, Libya, and Algeria.

²¹ these used to be called PROFORMA.

adversary's trap-doors on the Internet, thus rendering warfare obsolete. *IW/C2W is of little use in no-tech or low-tech environments.*

(3) National authorities will retain legal, policy, and regulatory authority regarding intrusion/ manipulation/ disruption of commercial telecommunications lines. Disruption of these lines, during war, will be under the purview of national strategic planners---and may be the subject of new international legal agreements.

(4) Advancements in computer technology offer the Commander of the Naval Expeditionary Task Force a double-edged sword: improved battlespace management by rapid delivery of actionable combat information regarding friendly and enemy forces, to both the operational decision makers and tactical commanders, but requiring confident protection by planning for "graceful degradation through effective but not restrictive security."²²

(5) IW/C2W for the Naval Expeditionary Force Commander should be approached at the operational planning level, using the same elements of operational design consistent with traditional principles of war.

²² paraphrased from "Information Architecture For The Battlefield" A Report of the Defense Science Board Summer Study Task Force, (OSD(A&T): Washington DC, 1994). p.6.

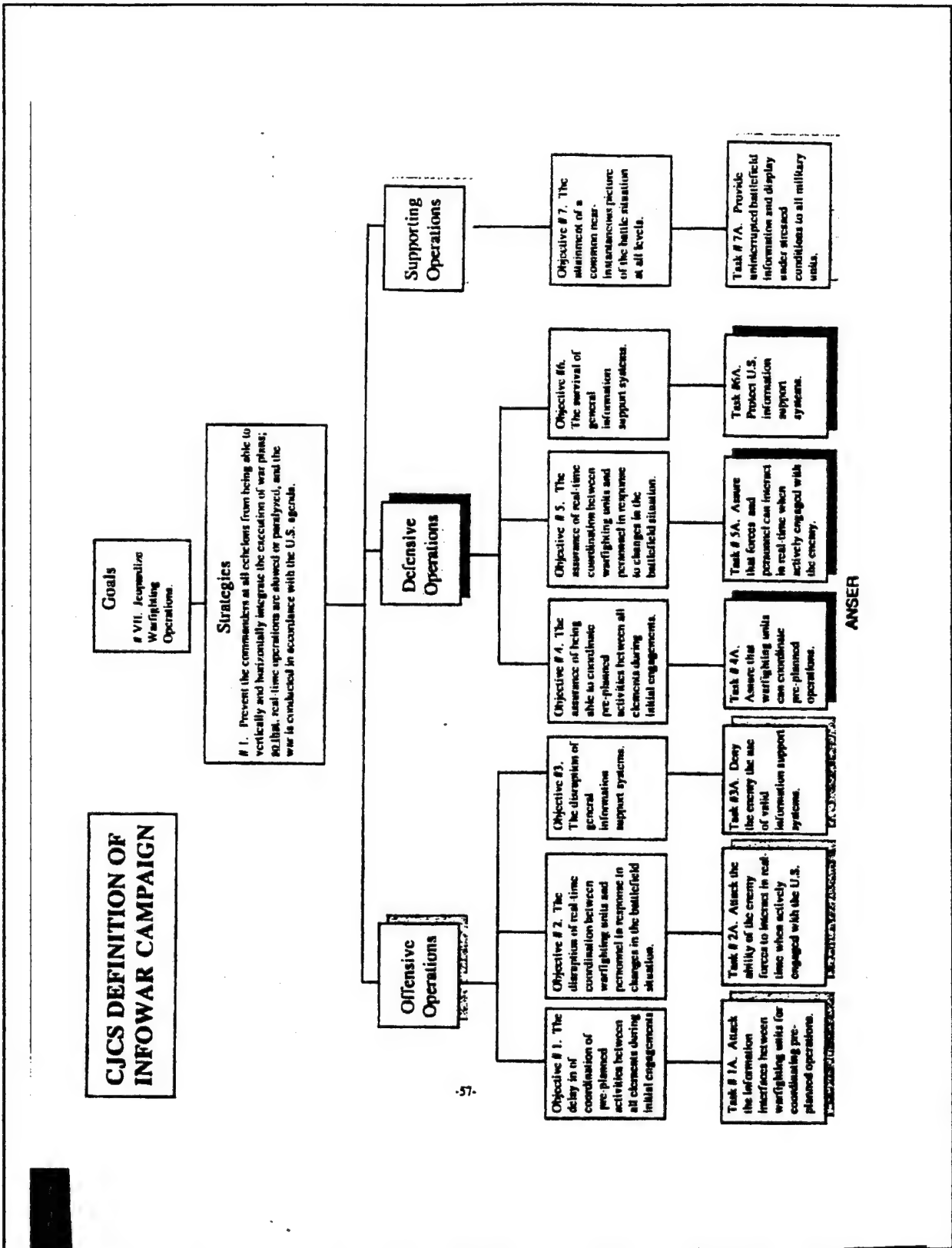
Cyberspace Weaponry²³

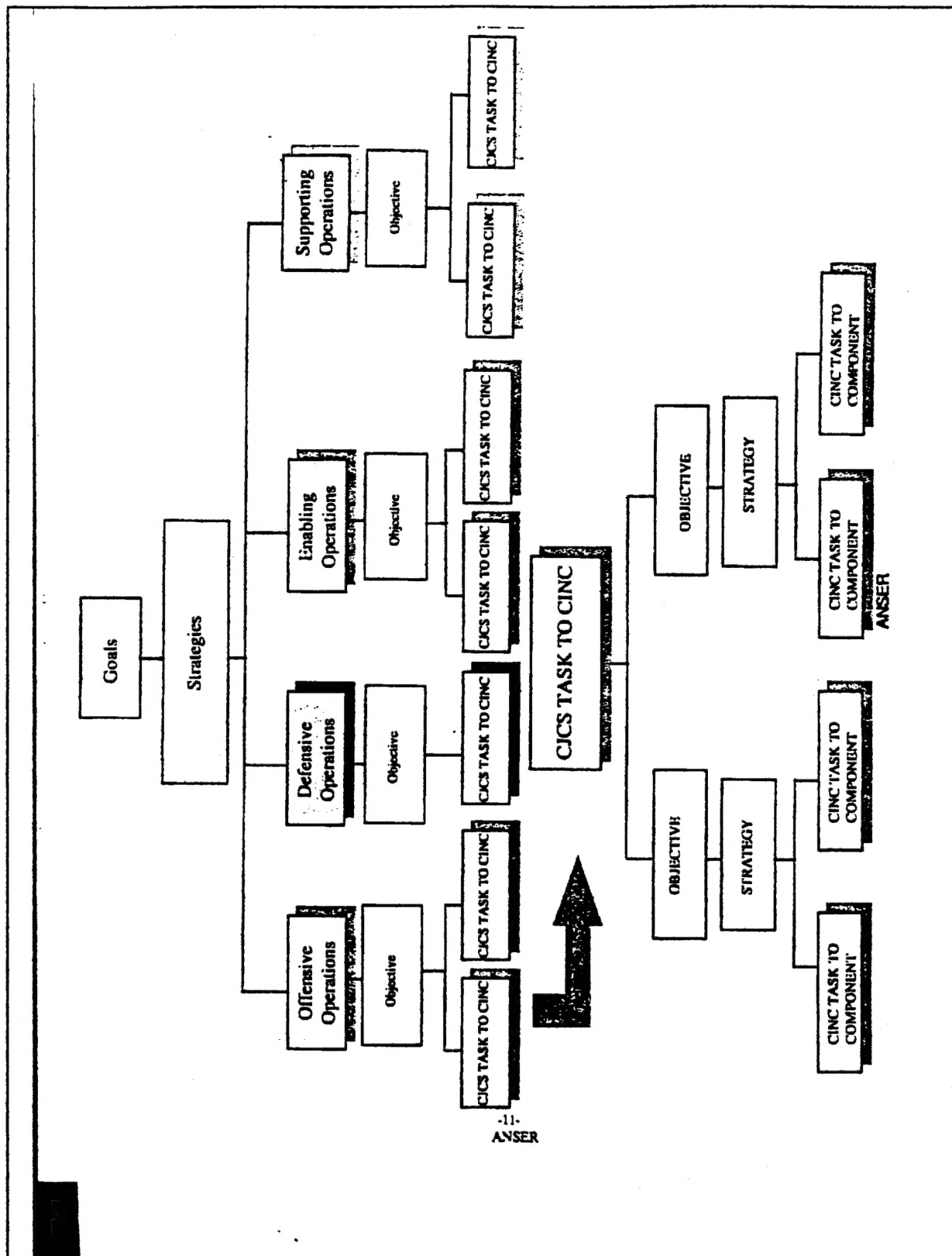
| | |
|---------------------------------|--|
| <i>Virus</i> | Programs that stealthily infect other programs, self-replicate, and spread within a computer system or network, some with anti-detection protection measures, may be encrypted, compressed or polymorphic to reduce detection. |
| <i>Covert channel</i> | A communications channel that takes advantage of system design flaws to allow information to be transmitted in a manner not intended to be possible, including covert storage channels and covert timing channels, that could be used to insert a virus. |
| <i>Data manipulation</i> | With the increasing capability to manipulate data comes opportunities to manipulate it for nefarious purposes; composition and content of pictures and data bases are vulnerable to advanced techniques. |
| <i>EMP bombs</i> | Electromagnetic pulse bombs can/erase damage data in memory, fuse circuits, or fry modems. |
| <i>Flaw</i> | An error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed; could be inserted by coherent RF weaponry, over a network from a remote site, or designed by an agent in place. |

²³ distilled from Julie Ryan and Gary Federico, "Offensive Information Warfare---A Concept Exploration" (Alexandra, Virginia: Center for Naval Analysis, 1994), p.4.

| | |
|--|--|
| <i>Logic bomb</i> | A piece of code buried within a larger computer system that executes when a specific state is realized. When executed, the bomb "explodes," erasing partial or total memory. |
| <i>Logic torpedo</i> | A virus, bomb or flaw aimed at one or more specific systems, released through cyberspace to hunt down its intended target. |
| <i>RF Weapon</i> | Because digital data is made up of ones and zeros (or ons and offs), a computer system can be affected by synchronous pulsing of electromagnetic energy at specified frequency ranges. This is known as bit flipping. Coherent RF weapons can be used to either distort data or insert viruses. Required to be close to the target, RF weapons can be inserted transmitters into the computer, or inserting modulation into the power supply or computer system. |
| <i>Time bomb</i> | Similar to a logic bomb, but different in that it detonates based on time rather than logic state. |
| <i>Time weapon</i> | Affecting the timing of internal computer clocks to throw off system synchronization, thereby affecting system internal and external communications. |
| <i>Trap door (or "back door")</i> | A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented, usually installed to allow system access to correct "bugs" in the operating system. |
| <i>Trojan Horse</i> | A program with an apparently useful function that performs other covert/secret functions, unbeknownst to the user (e.g. copying files). |

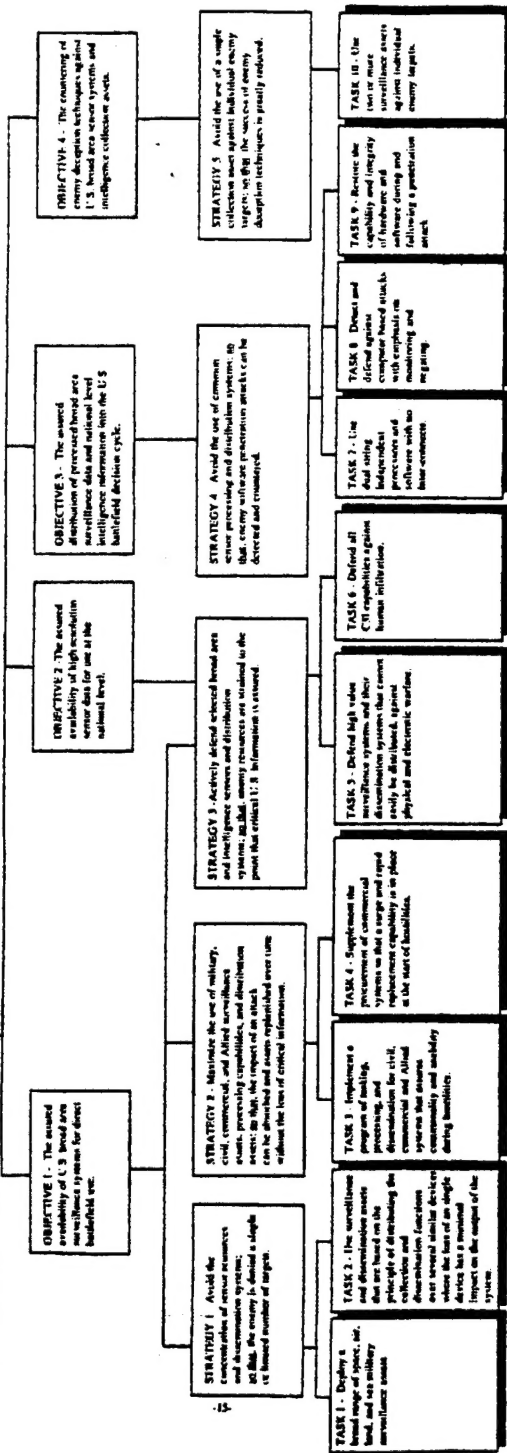
| | |
|---------------------|---|
| <i>Worms</i> | Similar to viruses, self-replicating at a rate that they prevent users gaining access to the system by overwhelming the system with the production of their progeny, can attack system availability, data integrity, or compromise confidentiality. |
|---------------------|---|





CJCS TASK #2A: PROTECT ALL ASPECTS OF THE U.S. C3I PROCESS AND INFRASTRUCTURE

CINC TASKING to the COMPONENTS



ANSER

BIBLIOGRAPHY

Books and Articles

- Evans, Gareth. "Cooperative Security and Intrastate Conflict," Foreign Policy, No. 10, Fall 1994.
- "Excerpts from Pentagon's Plan: "Prevent the Emergence of a New Rival," New York Times, March 8, 1992.
- Hutcherson, Norman B. (LTC/USAF), "Command and Control Warfare: Putting Another Tool in the Warfighter's Data Base," Maxwell AFB, AL: Air University Press, 1994
- Jones, Jefferey B. (COL/USA), "Psychological Operations in Desert Shield, Desert Storm, and Urban Freedom," Special Warfare, July 1994
- Posen, Barry R., and Ross, Andrew L. "Competing Grand Strategies," in Strategy and Force Planning Faculty, eds., "Strategy and Force Planning," Newport, RI: Naval War College Press, 1995.
- Schwartau, Winn, "Information Warfare," New York: Thunder's Point Press, 1994.
- Struble, Dan (LCDR/USN) "What is Command and Control Warfare?," Naval War College Review, Summer 1995.
- Toffler, Alvin, and Toffler, Heidi. "War and Anti-War: Survival at the Dawn of the 21st Century," New York: Little, Brown, and Company, 1993.

Published Reports and Instructions

- Aspin, Les, U.S. Dept. of Defense, "Report on the Bottom-Up Review", Washington, DC: October 1993.
- "Cryptology From The Sea," Commander, Naval Security Group Command, Washington DC, 1995.
- Defense Science Board Summer Task Force, "Information Architecture for the Battlefield," Office of the Under Secretary of Defense (Acquisition and Technology), The Pentagon, 1994.

Heimach, Charles E. "Regional Infowar Campaign: A Strategy to Task Breakout." ANSER: Arlington, VA, 1995.

Joint Chiefs of Staff, U.S. Dept. of Defense, "Command and Control Warfare", CJCS MOP 30, Washington DC: 8 March 1993.

Joint Chiefs of Staff, U.S. Dept. of Defense, "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance." Research Report for Chief, Information Warfare Division (J6K), Command, Control, and Computer Systems Directorate, The Joint Staff, Washington, DC, 4 July 1995.

Knecht, Ron, "Thoughts on Information Warfare," Science Applications International Corporation, June 1994

"National Security Strategy for Engagement and Enlargement." Washington, DC: The White House, Washington DC, February 1995.

"National Military Strategy of the United States of America: A Strategy of Flexible and Selective Engagement." The Joint Chiefs of Staff, The Pentagon, Washington DC, February 1995.

Ryan, Julie and Federico, Gary, "Offensive Information Warfare--A Concept Exploration." Center for Naval Analysis, Washington DC, 1994.

U.S. Navy Dept, "Information Warfare and Command and Control Warfare." OPNAVINST 3430.25, Washington DC: 1 April 1995.

U.S. Navy Dept, "Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W)", OPNAVINST 3430.26, Washington DC: 18 January 1995.